authentication data embedding portion 14 sets, similarly to the key data embedding portion 13, q to a nearest even or odd integer depending on the bit value of authentication data corresponding to the transform coefficient (step S704). Here, q is assumed to be a value obtained by dividing a transform coefficient by quantization step size Q.

Please amend the paragraph beginning on line 8 of page 32 as follows:

The key data determination portion 22 is not an indispensable component to the tamper detecting apparatus 2. In the present invention, however, such determination for verifying the key data improves reliability of the tamper detecting apparatus 2 in detection of ~~tamper~~ a tampering with the digital image. The key data determination portion 22 is therefore preferably used in view of making the tamper detecting apparatus 2 more preferable in practical use.

AMENDMENT TO THE CLAIMS:

1. (Currently amended) A tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal, said apparatus comprising:

a band division ~~means for dividing said~~ portion operable to divide the digital image signal into a plurality of frequency bands;

an authentication data generation ~~means for generating~~ portion operable to generate a pseudo-random number series by using predetermined key data, and ~~generating~~ to generate authentication data from the pseudo-random number series;

a key data embedding ~~means for embedding said~~ portion operable to embed the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among ~~said~~ the plurality of frequency bands;

an authentication data embedding ~~means for embedding said~~ portion operable to embed the authentication data in transform coefficients of the frequency bands exclusive of ~~said~~ the MRA

(hereinafter, referred to as MRR) among ~~said~~ the plurality of frequency bands; and

a band synthesis ~~means for reconstructing~~ portion operable to reconstruct the digital image signal in which the information has been embedded by using ~~said~~ the MRA and ~~said~~ the MRR to which data embedding processing is subjected.

2. (Currently amended) The tamper-detection-information embedding apparatus according to claim 1, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ and a set value m ~~(m is an integer not more than T)~~ are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size, ~~and~~

wherein said authentication data embedding ~~means~~ portion embeds ~~said~~ the authentication data in each transform coefficient of ~~said~~ the MRR by comparing an absolute value of ~~said~~ the transform coefficient with~~said~~ the set value T, and if the absolute value is less than ~~said~~ the set value T, setting the transform coefficient to ~~said~~ the set value +m or –m depending on a bit value of ~~said~~ the authentication data to be embedded, and if the absolute value is not less than ~~said~~ the set value T, setting the transform coefficient to an even or odd integer nearest to ~~said~~ the value q depending on the bit value of ~~said~~ the authentication data to be ~~embedded.~~ embedded. and

wherein T is a positive integer and m is an integer not more than T.

3. (Currently amended) A tamper detecting apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal, said tamper detecting apparatus comprising:

a band division ~~means for dividing said~~ portion operable to divide the digital image signal into a plurality of frequency bands;

a key data extraction ~~means for extracting~~ portion operable to extract key data embedded by ~~said~~ the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among ~~said~~ the plurality of frequency bands;

an authentication data generation ~~means for generating~~ portion operable to generate a pseudo-random number series by using ~~said~~ the key data, and ~~generating~~ to generate authentication data from the pseudo-random number series;

an embedded information extraction ~~means for extracting~~ portion operable to extract embedded information embedded based on ~~said~~ the key data by ~~said~~ the specific apparatus from transform coefficients of the frequency bands exclusive of ~~said~~ the MRA (hereinafter, referred to as MRR) among ~~said~~ the plurality of frequency bands; and

a tamper determination ~~means for comparing said~~ portion operable to compare the embedded information with ~~said~~ the authentication data for verification and ~~determining~~ to determine whether ~~said~~ the digital image has been tampered with.

4. (Currently amended) The tamper detecting apparatus according to claim 3, wherein said tamper determination ~~means~~ portion comprises:

a block division ~~means for dividing~~ portion operable to divide the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

a regional embedded information read ~~means for reading~~ portion operable to read, for each of ~~said~~ the unit blocks, embedded information embedded in the transform coefficients of ~~said~~ the MRR that represents the same spatial region as the unit block, serially from all of ~~said~~ the embedded information extracted by said embedded information extraction ~~means~~ portion;

a regional authentication data read ~~means for reading~~ portion operable to read, for each of ~~said~~ the unit blocks, authentication data corresponding in position to ~~said~~ the embedded information serially read by said regional embedded information read ~~means~~ portion, serially from all of ~~said~~ the authentication data generated by said authentication data generation ~~means~~ portion; and

a block-tamper determination ~~means for comparing said~~ portion operable to compare the embedded information serially read with ~~said~~ the authentication data serially read and ~~determining~~ to determine, for each of ~~said~~ the unit blocks, whether ~~said~~ the digital image has been tampered with.

5. (Currently amended) The tamper detecting apparatus according to claim 3, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ is predetermined and q is predetermined as a value obtained by dividing a transform coefficient ~~is~~ by a predetermined quantization step size and then rounding off the result, ~~and~~

wherein said embedded information extraction ~~means~~ portion extracts ~~said~~ the embedded information from each transform coefficient of ~~said~~ the MRR by comparing an absolute value of ~~said~~ the transform coefficient with ~~said~~ the set value T, and if the absolute value is less than ~~said~~ the set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and if the absolute value is not less than ~~said~~ the set value T, determining whether ~~said~~ the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination.~~ determination, and

wherein T is a positive integer.

6. (Currently amended) The tamper detecting apparatus according to claim 4, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result, ~~and~~

wherein said embedded information extraction ~~means~~ portion extracts ~~said~~ the embedded information from each transform coefficient of ~~said~~ the MRR by comparing an absolute value of ~~said~~ the transform coefficient with ~~said~~ the set value T, and if the absolute value is less than ~~said~~ the set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and if the absolute value is not less than ~~said~~ the set value T, determining whether ~~said~~ the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination.~~ determination, and

wherein T is a positive integer.

7. (Currently amended) A tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal, said method comprising:

~~a step of~~ dividing ~~said~~ the digital image signal into a plurality of frequency bands;

~~a step of~~ generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series;

~~a step of~~ embedding ~~said~~ the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among ~~said~~ the plurality of frequency bands;

~~a step of~~ embedding ~~said~~ the authentication data in transform coefficients of the frequency bands exclusive of ~~said~~ the MRA (hereinafter, referred to as MRR) among ~~said~~ the plurality of frequency bands; and

~~a step of~~ reconstructing the digital image signal in which the information has been embedded by using ~~said~~ the MRA and ~~said~~ the MRR to which data embedding processing is subjected.

8. (Currently amended) The tamper-detection-information embedding method according to claim 7, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ and a set value m ~~(m is an integer not more than T)~~ are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size, ~~and~~

~~said step of~~ wherein embedding authentication data ~~includes:~~ includes

~~a step of~~ comparing an absolute value of ~~said~~ the transform coefficient with ~~said~~ the set value T;

~~a step of~~ setting the transform coefficient to ~~said~~ the set value +m or –m depending on a bit value of ~~said~~ the authentication data to be embedded if the absolute value is less than ~~said~~ the set value ~~T;~~ T, and

~~a step of~~ setting the transform coefficient to an even or odd integer nearest to ~~said~~ the value q depending on the bit value of ~~said~~ the authentication data to be embedded if the absolute value is not less than ~~said~~ the set value ~~T.~~ T, and

wherein T is a positive integer and m is an integer not more than T.

9. (Currently amended) A tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal, said method comprising:

~~a step of~~ dividing ~~said~~ the digital image signal into a plurality of frequency bands;

~~a step of~~ extracting key data embedded by ~~said~~ the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among ~~said~~ the plurality of frequency bands;

~~a step of~~ generating a pseudo-random number series by using ~~said~~ the key data, and generating authentication data from the pseudo-random number series;

~~a step of~~ extracting embedded information embedded based on ~~said~~ the key data by ~~said~~ the specific apparatus from transform coefficients of the frequency bands exclusive of ~~said~~ the MRA (hereinafter, referred to as MRR) among ~~said~~ the plurality of frequency bands; and

~~a step of~~ comparing ~~said~~ the embedded information with ~~said~~ the authentication data for verification and determining whether ~~said~~ the digital image has been tampered with.

10. (Currently amended) The tamper detecting method according to claim 9, ~~wherein~~ further comprising

~~said step of determining tamper comprises:~~

~~a step of~~ dividing the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

~~a step of~~ reading, for each of ~~said~~ the unit blocks, embedded information embedded in the transform coefficients of ~~said~~ the MRR that represents the same spatial region as the unit block, serially from all of ~~said~~ the embedded information;

~~a step of~~ reading, for each of ~~said~~ the unit blocks, authentication data corresponding in position to ~~said~~ the embedded information serially read, serially from all of ~~said~~ the authentication data; and

~~a step of~~ comparing a series of ~~said~~ the embedded information serially read with a series of ~~said~~ the authentication data serially read and determining, for each of ~~said~~ the unit blocks, whether ~~said~~ the digital image has been tampered with.

11. (Currently amended) The tamper detecting method according to claim 9, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result, ~~and~~

wherein said ~~step of~~ extracting embedded information ~~includes:~~ includes

~~a step of~~ comparing an absolute value of ~~said~~ the transform coefficient with ~~said~~ the set value ~~T;~~ T,

~~a step of~~ determining whether a value of the transform coefficient is positive or negative if the absolute value is less than ~~said~~ the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination;~~ determination, and

~~a step of~~ determining whether ~~said~~ the value q is even or odd if the absolute value is not less than ~~said~~ the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination.~~ determination, and

wherein T is a positive integer.

12. (Currently amended) The tamper detecting method according to claim 10, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result, ~~and~~

wherein said ~~step of~~ extracting embedded information ~~includes:~~ includes

~~a step of~~ comparing an absolute value of ~~said~~ the transform coefficient with ~~said~~ the set value ~~T;~~ T,

~~a step of~~ determining whether a value of the transform coefficient is positive or negative if the absolute value is less than ~~said~~ the set value T, and extracting a bit value of embedded

information embedded in the transform coefficient based on the ~~determination;~~ determination, and

~~a step of~~ determining whether ~~said~~ the value q is even or odd if the absolute value is not less than ~~said~~ the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination.~~ determination, and

wherein T is a positive integer.

13. (Currently amended) A recording medium on which a program having computer device readable instructions to be run on a computer device is recorded for carrying out a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal, the ~~method comprising the steps of~~ computer device readable instructions including instructions capable of instructing a computer device to perform the method comprising:

dividing ~~said~~ the digital image signal into a plurality of frequency bands;

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series;

embedding ~~said~~ the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among ~~said~~ the plurality of frequency bands;

embedding ~~said~~ the authentication data in transform coefficients of the frequency bands exclusive of ~~said~~ the MRA (hereinafter, referred to as MRR) among ~~said~~ the plurality of frequency bands; and

reconstructing the digital image signal in which the information has been embedded by using ~~said~~ the MRA and ~~said~~ the MRR to which data embedding processing is subjected.

14. (Currently amended) The recording medium according to claim 13, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ and a set value m ~~(m is an integer not more than T)~~ are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size, ~~and~~

wherein said ~~step of~~ embedding authentication data includes ~~the steps of~~:

comparing an absolute value of ~~said~~ the transform coefficient with ~~said~~ the set value ~~T;~~ T,

setting the transform coefficient to ~~said~~ the set value +m or –m depending on a bit value of ~~said~~ the authentication data to be embedded if the absolute value is less than ~~said~~ the set value ~~T;~~ T, and

setting the transform coefficient to an even or odd integer nearest to ~~said~~ the value q depending on the bit value of ~~said~~ the authentication data to be embedded if the absolute value is not less than ~~said~~ the set value ~~T.~~ T, and

wherein T is a positive integer and m is an integer not more than T.

15. (Currently amended) A recording medium on which a program having computer device readable instructions to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal, the ~~method comprising the steps of~~ computer device readable instructions including instructions capable of instructing a computer device to perform the method comprising:

dividing ~~said~~ the digital image signal into a plurality of frequency bands;

extracting key data embedded by ~~said~~ the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among ~~said~~ the plurality of frequency bands;

generating a pseudo-random number series by using ~~said~~ the key data, and generating authentication data from the pseudo-random number series;

extracting embedded information embedded based on ~~said~~ the key data by ~~said~~ the specific apparatus from transform coefficients of the frequency bands exclusive of ~~said~~ the MRA (hereinafter, referred to as MRR) among ~~said~~ the plurality of frequency bands; and

comparing ~~said~~ the embedded information with ~~said~~ the authentication data for verification and determining whether ~~said~~ the digital image has been tampered with.

16. (Currently amended) The recording medium according to claim 15, wherein ~~said step of determining tamper comprises~~ the computer device readable instructions include instructions capable of instructing a computer device to perform the method further comprising:

dividing the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

reading, for each of ~~said~~ the unit blocks, embedded information embedded in the transform coefficients of ~~said~~ the MRR that represents the same spatial region as the unit block, serially from all of ~~said~~ the embedded information;

reading, for each of ~~said~~ the unit blocks, authentication data corresponding in position to ~~said~~ the embedded information serially read, serially from all of ~~said~~ the authentication data; and

comparing a series of ~~said~~ the embedded information serially read with a series of ~~said~~ the authentication data serially read and determining, for each of ~~said~~ the unit blocks, whether ~~said~~ the digital image has been tampered with.

17. (Currently amended) The recording medium according to claim 15, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ is predetermined and q is predetermined as a value obtained by dividing a transform coefficient is divided by a predetermined quantization step size and then rounding off the result, ~~and~~

wherein said ~~step of~~ extracting embedded information includes ~~the steps of:~~

comparing an absolute value of ~~said~~ the transform coefficient with ~~said~~ the set value ~~T:~~ T.

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than ~~said~~ the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination:~~ determination, and

determining whether ~~said~~ the value q is even or odd if the absolute value is not less than ~~said~~ the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination.~~ determination, and

wherein T is a positive integer.

18. (Currently amended) The recording medium according to claim 16, ~~wherein~~

wherein a set value T ~~(T is a positive integer)~~ is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result, ~~and~~

wherein said ~~step of~~ extracting embedded information includes ~~the steps of:~~

comparing an absolute value of ~~said~~ the transform coefficient with ~~said~~ the set value ~~T;~~ T,

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than ~~said~~ the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination;~~ determination, and

determining whether ~~said~~ the value q is even or odd if the absolute value is not less than ~~said~~ the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the ~~determination.~~ determination, and

wherein T is a positive integer.